L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno. Per questo motivo:

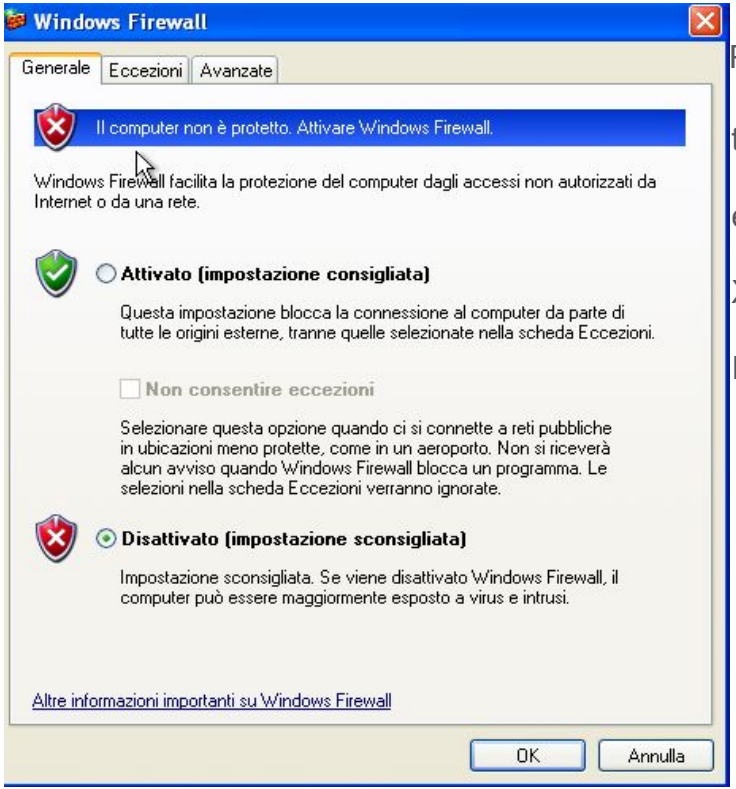
● Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP.

● Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection).

● Abilitare il Firewall sulla macchina Windows XP.

● Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Questa era la traccia dell’ esercizio di oggi.
Il primo passaggio è stato assicurarsi che il Firewall di Windows XP, come richiesto dalla traccia, fosse disattivato:



Poi, da Kali Linux, ho avviato una prima scansione su Windows XP tramite nmap (avevo precedentemente cambiato gli indirizzi IP di entrambe le macchine (Kali ha indirizzo IP **192.168.240.100**, Windows XP **192.168.240.150**).

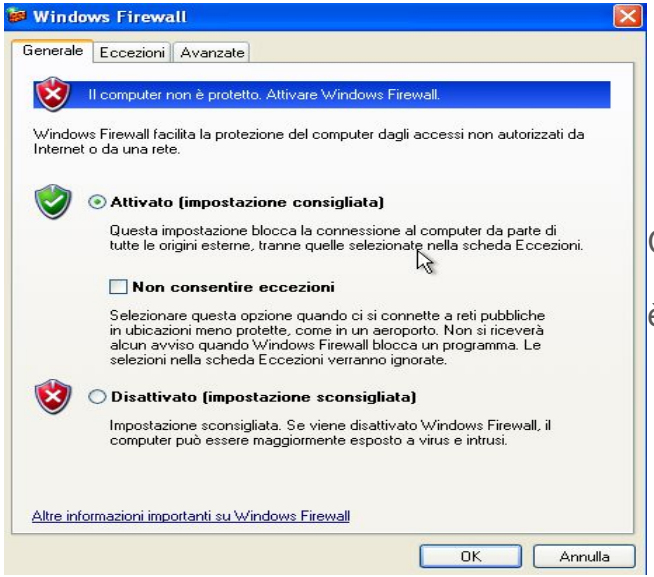
Il comando per far partire la scansione è **nmap -sV 192.168.240.150**

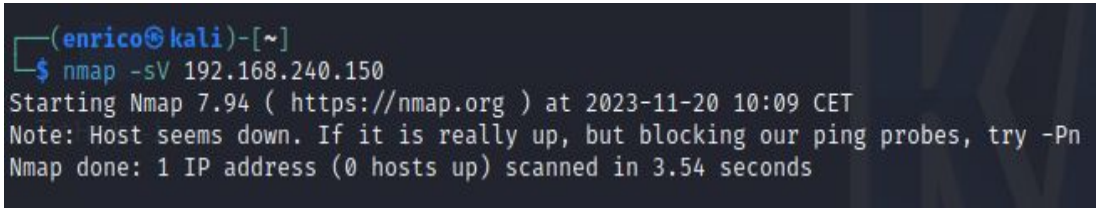
```
┌──(enrico㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 10:07 CET
Nmap scan report for 192.168.240.150
Host is up (0.00050s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds
```

Come visibile dalla slide della scansione, le uniche porte rilevate da nmap sono la **135**, **139** e **445**, dei cui servizi attivi abbiamo anche la versione in uso. Nmap non ha mostrato le altre **997** porte (per raggiungere almeno le 1000 più comunemente utilizzate). Questo, nonostante il Firewall di Windows XP sia disattivato, può essere dovuto al fatto che non ci siano servizi in ascolto su tutte le altre porte. Un motivo correlato a questo potrebbe essere che, essendo Windows XP un sistema operativo vecchio, è probabile che alcuni dei servizi più comuni non siano installati o aggiornati.

A questo punto ho abilitato il Firewall su Windows XP, e ho fatto partire una nuova scansione sulla macchina XP:





Come vediamo da questa nuova scansione, ora nmap ci comunica che l'host è down o che, se è up, sta bloccando i tentativi di ping del programma.

Questo perchè nmap tenta di determinare se un host è attivo utilizzando il protocollo **ICMP** (ping), mentre il firewall è configurato per bloccare i pacchetti di dati non autorizzati o sospetti, inclusi quelli provenienti dalla scansione di nmap che sono effettivamente dei ping sull' host. Ecco perchè, nonostante l' host (Windows XP) sia effettivamente attivo, nmap ce lo segnala come **down** e non riesce a darci informazioni sulle porte aperte e sui servizi in ascolto su di esse.

```
┌──(enrico㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 10:10 CET
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 16.50% done; ETC: 10:14 (0:02:52 remaining)
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 37.00% done; ETC: 10:14 (0:02:08 remaining)
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 64.50% done; ETC: 10:14 (0:01:12 remaining)
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.59 seconds
```

Ho quindi fatto una terza scansione, aggiungendo **-Pn** al comando di nmap per poter saltare il protocollo ICMP (quindi non determina se l' host è attivo o meno, ma si concentra direttamente sulla scansione delle porte. Tuttavia, essendo il Firewall attivo, la risposta che otteniamo dalla scansione è che tutte le 1000 porte scansionate sul sistema target sono in **ignored states**, ovvero il Firewall sta funzionando esattamente come dovrebbe funzionare per bloccare tentativi di connessione non autorizzati.